1

Capitolo B42
numeri reali

Contenuti delle sezioni

B420.01 Questo capitolo è dedicato ad una introduzione assiomatica "morbida", che non richiede astrazioni lontane della intuizione spaziale, dell'insieme dei numeri reali, l'insieme numerico che intuitivamente si presenta assimilandolo alla linea retta della geometria classica con il fine, in particolare, di utilizzarlo come base base per la formalizzazione della nozione di continuità.

Dopo aver introdotti i numeri reali costruibili [B38], si trova necessario un ulteriore ampliamento delle entità numeriche che non discende da esigenze computazionali, ma da una sentita opportunità sul piano della organizzazione dell'*esposizione*: si reputa molto vantaggiosa una nozione astratta di un insieme numerico totalmente ordinato che consenta di formalizzare in modo logicamente soddisfacente le molte argomentazioni di portata generale richieste per introdurre e utilizzare le nozioni di limite, continuità e derivabilità.
Inoltre l'impostazione assiomatica consente di trattare efficacemente le numerose funzioni studiate nell'analisi matematica, soprattutto collegandole ad equazioni nelle quali intervengano, oltre alle operazioni algebriche, costruzioni infinitesimali come derivazione e integrazione e successivamente consente di affrontare efficacemente tutte le loro applicazioni che si servono di modelli continui.

B420.02 L'insieme dei numeri reali $\mathbb{R}$ viene introdotto come terreno di un campo ordinato mediante assiomi che, facendo riferimento a operazioni e a una relazione d'ordine ampiamente praticate e comunemente visualizzate, possono essere supportati dall'intuizione e ampiamente condivisi.
Dagli assiomi si ricava che tre sottoinsiemi propri di $\mathbb{R}$ si possono identificare con l'insieme dei razionali, con l'insieme dei numeri algebrici e con l'insieme dei numeri reali costruibili, i tre insiemi numerici introdotti per soddisfare esigenze computazionali molto sentite.

I numeri reali si possono quindi vedere come estensione-idealizzazione dei numeri reali costruibili la quale consente di migliorare decisamente l'organizzazione delle conoscenze matematiche, miglioria evidente innanzi tutto nella presentazione dell'analisi matematica [tomo I].

B42 a. campi completi secondo Dedekind e campi archimedei

B42a.01 Premettiamo due importanti caratteristiche dei campi ordinati.

Consideriamo un insieme $\boldsymbol{R}$ munito da una relazione d'ordine $\leq$ (non necessariamente totale). Si dice che l'insieme ordinato $\langle \boldsymbol{R}, \leq \rangle$ soddisfa la **proprietà di completezza di Dedekind**, ovvero che è completo secondo Dedekind, sse per ogni suo sottoinsieme $\boldsymbol{S}$ superiormente limitato contiene il suo estremo superiore, cioè il minimo dei suoi maggioranti, ovvero sse $\sup(\boldsymbol{S}) \in \boldsymbol{S}$.

La proprietà di completezza di Dedekind interessa innanzi tutto per i campi ordinati.

Chiaramente il campo dei razionali non è completo secondo Dedekind; sono molti i sottoinsiemi di $\mathbb{Q}$ superiormente limitati che non possiedono un estremo superiore razionale: per esempio gli insiemi dei razionali positivi con il quadrato minore di ciascuno degli interi positivi che non sono quadrati di interi (2, 3, 5, 6, 7, 8, 10, 11, ...).

Neppure il campo dei numeri algebrici è completo secondo Dedekind; ad esempio si dimostra che non sono numeri algebrici gli estremi superiori dei seguenti insiemi di numeri (razionali e quindi) algebrici

$$\left\{ n \in \mathbb{N} : \middle| \sum_{i=0}^{n} \frac{1}{i!} \right\} \quad , \qquad \left\{ n \in \mathbb{N} : \middle| \left(1 + \frac{1}{n}\right)^n \right\} \quad ,$$

$$\left\{ 1 \ , \ \ 1 - \frac{1}{3} \ , \ \ 1 - \frac{1}{3} + \frac{1}{5} \ , \ \ 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \ , \ \ 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} \ , \ \ ... \right\}$$

$$\left\{ \frac{1}{1 \cdot 3} \ , \ \ \frac{1}{1 \cdot 3} + \frac{1}{5 \cdot 7} \ , \ \ \frac{1}{1 \cdot 3} + \frac{1}{5 \cdot 7} + \frac{1}{9 \cdot 11} \ , \ \ \frac{1}{1 \cdot 3} + \frac{1}{5 \cdot 7} + \frac{1}{9 \cdot 11} + \frac{1}{13 \cdot 15} \ , \ \ ... \right\}$$

B42a.02 Esaminiamo ora un campo totalmente ordinato $\boldsymbol{R} = \langle R, +, -, \odot, ^{-1}, 0, 1, \leq \rangle$.

Si dicono **elementi positivi del campo $\boldsymbol{R}$** gli elementi x di R tali che $0 \leq x$.

Consideriamo due diversi elementi positivi x e y e più particolarmente supponiamo sia $x < y$; i due elementi si dicono **elementi del campo confrontabili** sse si trova un intero positivo n tale che $n \cdot x > y$; se al contrario per ogni intero positivo n si ha $n \cdot x < y$ si dice che x è **elemento relativamente infinitesimo** rispetto a y.

Risulta in tal modo individuata la relazione "essere relativamente infinitesimo in un campo ordinato".

Si dice che il campo totalmente odinato $\boldsymbol{R}$ gode della **proprietà di Archimede**, o equivalentemente che $\boldsymbol{R}$ è un **campo archimedeo** sse ogni duetto dei suoi elementi è costituito da elementi confrontabili.

Dati due numeri razionali positivi qualsiasi $\frac{p}{q}$ e $\frac{r}{s}$, si sa stabilire se $\frac{p}{q} < \frac{r}{s}$: basta constatare se $p\,s < q\,r$ o meno.
Dato che ovviamente $1 < p\,s, q\,r$, si può assumere $n := \left\lceil \frac{q}{r} \right\rceil$ per ottenere $n\frac{p}{s} > \frac{q}{r}$ e quindi concludere che $\mathbb{Q}$ costituisce un campo archimedeo.

Di conseguenza sono archimedei anche il campo dei numeri algebrici ed il campo dei numeri reali costruibili, campi dei quali l'insieme dei razionali è un sottoinsieme denso.

B42a.03 Un notevole esempio di campo totalmente ordinato nonarchimedeo è fornito dal campo FunQtQ_{Fld} avente come terreno l'insieme FunQtQ delle funzioni in una variabile fornite da una espressione razionale (nella quale compaiono solo costanti razionali) che quindi a ogni valore razionale della variabile associano un valore razionale.

A ciascuna di queste funzioni si può dare la forma $P(x) + \dfrac{N(x)}{D(x)}$ con $P(x)$, $N(x)$ e $D(x)$ polinomi con coefficienti razionali, con $deg(N(x)) < deg(D(x))$ e con $D(x)$ monico.

Una tale funzione $f(x) = P(x) + \dfrac{N(x)}{D(x)}$ si considera positiva sse è positivo il coefficiente dominante di $P(x)$ oppure si ha $P(x) = 0$ e, assunto positivo il coefficiente dominante di $D(x)$, è positivo il coefficiente dominante di $N(x)$.
Per affermare che una funzione $f(x) \in \mathsf{FunQtQ}$ è positiva scriviamo $0_f \prec_{QF} f(x)$, intendendo che sia $0_f := \lceil x \in \mathbb{Q} \mapsto 0 \rceil$.

Date due funzioni $r(x), s(x) \in \mathsf{FunQtQ}$, si stabilisce che $r(x) \prec_{QF} s(x)$ sse $0_f \prec_A s(x) - r(x)$.

la relazione d'ordine $\preceq_{QF} := \prec_{QF} \dot\cup \mathsf{Id}_{FunQtQ}$ è evidentemente una relazione d'ordine totale e, munito di essa il campo FunQtQ_{Fld} costituisce un campo totalmente ordinato che denotiamo con $\mathsf{FunQtQ}_{Fld;\preceq_A}$.

Infatti, due funzioni razionali qualsiasi

$$f_1(x) := P_1(x) + \frac{N_1(x)}{D_1(x)} \quad \text{e} \quad f_2(x) = P_2(x) + \frac{N_2(x)}{D_2(x)} ,$$

per le quali si assume che abbiano positivo il coefficiente dominante sia $D_1(x)$ che $D_2(x)$, si possono confrontare con l'algoritmo che segue.

Si confrontano $P_1(x)$ e $P_2(x)$.
    se $P_1(x) \prec_{QF} P_2(x)$ si conclude $f_1 \prec_{QF} f_2(x)$;
    se $P_2(x) \prec_{QF} P_1(x)$ si conclude $f_2 \prec_{QF} f_1(x)$;
    se altrimenti si confrontano $N_1(x$ e $N_2(x)$;
    se $N_1(x) \prec_{QF} N_2(x)$ si conclude $f_1 \prec_{QF} f_2(x)$;
    se $N_2(x) \prec_{QF} N_1(x)$ si conclude $f_2 \prec_{QF} f_1(x)$;
    se altrimenti si confrontano $D_1(x)$ e $D_2(x)$;
        se $D_1(x) \prec_{QF} D_2(x)$ si conclude $f_2 \prec_{QF} f_1(x)$;
        se $D_2(x) \prec_{QF} D_1(x)$ si conclude $f_1 \prec_{QF} f_2(x)$;
        se altrimenti deve essere $f_1(x) = f_2(x)$.

In particolare la funzione $1/x$ è minore della funzione costante 1 e per qualsiasi intero positivo n si ha $n \cdot 1/x \prec_{QF} 1$; quindi il campo ordinato $\mathsf{FunQtQ}_{Fld;\preceq_{QF}}$ è nonarchimedeo.

In termini colloquiali possiamo dire che in un campo archimedeo non si possono individuare elementi positivi con le caratteristiche delle quantità infinitesime.

Si constata che si ottengono campi nonarchimedei individuando relazioni di ordine totale definibili a partire da cascata di più relazioni d'ordine totale archimedee infinite.

B42 b. introduzione formale dei numeri reali

B42b.01 Diciamo **campo dei numeri reali** la struttura algebrico-relazionale della forma

$$\mathbb{R}_{Fld} = \langle \mathbb{R}, +, -, 0, \cdot, 1, ^{-1}, \leq \rangle$$

che soddisfa le richieste che seguono.

[Re 1] $\langle \mathbb{R}, +, -, 0, \cdot, 1, ^{-1} \rangle$ è un campo; questo equivale ad affermare quanto segue.

(a) $+$ è un'operazione binaria su $\mathbb{R}$ chiamata somma tale che

(i) $\forall x, y \in \mathbb{R} \,:\, x + y = y + x$ (la somma è commutativa);

(ii) $\forall x, y, z \in \mathbb{R} \,:\, x + (y + z) = (x + y) + z$ (la somma è associativa);

(b) 0 è l'elemento neutro per la somma, cioè $\forall x \in \mathbb{R} \,:\, x + 0 = x$;

(c) $-$ è l'operazione di passaggio all'inverso per la somma, cioè $\forall x \in \mathbb{R} \,:\, x + (-x) = 0$;

(d) $\cdot$ è un'operazione binaria su $\mathbb{R}$ chiamata prodotto tale che

(i) $\forall x, y \in \mathbb{R} \,:\, x \cdot y = y \cdot x$ (il prodotto è commutativo);

(ii) $\forall x, y, z \in \mathbb{R} \,:\, x \cdot (y \cdot z) = (x \cdot y) \cdot z = x$ (il prodotto è associativo);

(e) 1 è diverso da 0 ed è l'elemento neutro per il prodotto, cioè $\forall x \in \mathbb{R} \;:\; 1 \cdot x = x$;

(f) $^{-1}$ è l'operazione di passaggio all'inverso per il prodotto, ma limitatamente a $\mathbb{R}_{nz} := \mathbb{R} \setminus \{0\}$, cioè $\forall x \in \mathbb{R}_{nz} \,:\, x \cdot x^{-1} = 1$;

(g) il prodotto è distributivo rispetto alla somma, cioè $\forall x, y, z \in \mathbb{R} \,:\, x \cdot (y + z) = x \cdot y + x \cdot z$;

[Re 2] $\langle \mathbb{R}, \leq \rangle$ è un insieme totalmente ordinato, cioè

(a) $\forall x \in \mathbb{R} \,:\, x \leq x$ (riflessività);

(b) $\forall x, y \in \mathbb{R} \,:\, x \leq y, y \leq x \Longrightarrow x = y$ (antisimmetria);

(c) $\forall x, y, z \in \mathbb{R} \,:\, x \leq y, y \leq z \Longrightarrow x \leq z$ (transitività);

(d) $\forall x, y \in \mathbb{R} \;:\; x \leq y \;\vee\; y \leq x$ (totalità dell'ordine).

[Re 3] Le operazioni $+$ e $\cdot$ si dicono **operazioni compatibili con l'ordine** in quanto

(a) $\forall x, y, z \in \mathbb{R} \;:\; x \leq y \Longrightarrow x + z \leq y + z$ (mantenimento dell'ordine da parte della somma);

(b) $\forall x, y, z \in \mathbb{R} \;:\; 0 \leq x \leq y, 0 \leq z \Longrightarrow x \cdot y \leq y \cdot z$;

(mantenimento dell'ordine da parte del prodotto).

[Re 4] L'ordine soddisfa l'**assioma di Archimede**: denotando con $\mathbb{R}_+$ l'insieme degli elementi di $\mathbb{R}$ maggiori di 0 e con $\mathbb{R}_{0+} := \mathbb{R}_+ \cup \{0\}$, si ha $\forall x \in \mathbb{R}_+ \,,\; y \in \mathbb{R}_{0+} \,:\, \mathbb{P} \ni n \;]\!\!]\; y \leq nx$.

A questo punto si può affermare che $\mathbb{R}_{Fld}$ è un campo totalmente ordinato archimedeo.

Inoltre si possono definire come intervalli chiusi finiti di numeri reali gli insiemi associati a coppie di numeri reali $\langle a, b \rangle$ con $a \leq b \searrow$ **[**a,b **]** $:= \{x \in \mathbb{R} \;]\!\!]\; a \leq x \leq b\}$.

Definiamo **successione di intervalli reali chiusi annidati**, in sigla srni,

ogni $\big\langle n \in \mathbb{N} :| \,[a_n, b_n]\big\rangle$ tale che $\forall n \in \mathbb{N} \,:\, a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$.

In particolare definiamo **successione di intervalli reali chiusi annidati convergente**, in breve srnic,

ogni `srni` $\big\langle n \in \mathbb{N} :| \,[a_n, b_n]\big\rangle$ tale che $\lim_{n \to +\infty} b_n - a_n = 0$.

[Re 5] Vale l'**assioma degli intervalli annidati**:

l'intersezione di ogni successione di intervalli reali chiusi annidati non è vuota.

Possiamo anche aggiungere che l'ordine $\leq$ è completo secondo Dedekind, ossia ogni S sottoinsieme nonvuoto di $\mathbb{R}$ limitato superiormente contiene un elemento u (suo estremo superiore) tale che per ogni v maggiorante di S si ha $u \leq v$.

B42 c. proprietà di ordinamento dell'insieme dei reali

B42c.01 In questa sezione vengono dedotte dagli assiomi precedenti le proprietà di ordinamento dell'insieme dei numeri reali.

Molte di queste sono intuitive quando si pensa $\mathbb{R}$ in corrispondenza biunivoca con i punti di una retta orizzontale nella quale sono privilegiati due punti diversi, il primo chiamato origine e il secondo, alla sua destra, la cui distanza dall'origine si assume uguale ad 1; questo equivale a scegliere la distanza tra i due punti come unità di misura delle distanze tra punti della retta.

Ci proponiamo inoltre di identificare gli insiemi degli interi, dei razionali e dei reali costruibili con sottoinsiemi di $\mathbb{R}$.

Nel seguito con r, s, t, r_i, s_i per $i = 0, 1, 2, 3, ...$ denoteremo numeri reali.

B42c.02 Introduciamo la scrittura $r < s$, da leggere "r è minore di s", come equivalente alla affermazione $\ulcorner r \leq s \;\wedge\; r \neq s \urcorner$. In altre parole si introduce la relazione "$<$" come riduzione antiriflessiva della "$\leq$".

(1) Prop.: (**proprietà tricotomica**)

Dati due numeri reali r ed s, allora $\ulcorner$ aut $r < s$, aut $r = s$, aut $r > s \urcorner$.

Dim.: Discende da [Re 2](d) dopo aver escluso che sia $r = s$ ▮

(2) Prop.: $r \leq s \;\wedge\; s < t \implies r < t \quad , \quad r < s \;\wedge\; s \leq t \implies r < t$ ▮

(3) Prop.: Ogni sottoinsieme finito di $\mathbb{R}$ possiede un minimo e un massimo.

Dim.: Da (1) segue per i duetti, ossia per sottoinsiemi di due elementi; quindi si estende per ricorrenza ai sottoinsiemi con più di due elementi ▮

(4) Prop.: Ogni sottoinsieme di $n = 2, 3, ...$ elementi di $\mathbb{R}$ si può porre in biiezione con (n].

Dim.: Anche questo enunciato si ottiene per ricorrenza sul numero degli elementi del sottoinsieme ▮

B42c.03 **(1) Prop.:** Sia $n = 2, 3, 4, ...$ e si abbiano due sequenze di numeri reali $\langle r_1, r_2, ..., r_n \rangle$ e $\langle s_1, s_2, ..., s_n \rangle$;

(a) $\ulcorner \forall i = 1, ..., n \;\colon\; r_i \leq s_i \urcorner \implies r_1 + \cdots + r_n \;\leq\; s_1 + \cdots + s_n$;

(b) $\ulcorner \ulcorner \forall i = 1, ..., n \;\colon\; r_i \leq s_i \urcorner \;\wedge\; \ulcorner$ per almeno un $j \in$ (n] si ha $r_j < s_j \urcorner \urcorner$

$\implies r_1 + \ldots + r_n \;<\; s_1 + \cdots + s_n$.

Dim.: Si ottengono per induzione su n ▮

(2) Prop.: $\forall t \in \mathbb{R} \;\colon\; r \leq s \iff r + t \leq s + t \quad ; \quad \forall t \in \mathbb{R} \;\colon\; r < s \iff r + t < s + t$ ▮

(3) Prop.: $r \leq s \iff 0 \leq s - r \iff -s \leq -r \quad ; \quad r < s \iff 0 < s - r \iff -s < -r$ ▮

(4) Prop.: $r \geq 0 \iff \forall n \in \mathbb{P} \colon nr \geq 0; \qquad r > 0 \iff \forall n \in \mathbb{P} \colon nr > 0$ ▮

B42c.04 Se $r < s$ si definiscono i seguenti **intervalli reali finiti**

$[r, s] := \{t \in \mathbb{R} \mid r \leq t \leq s\}$ (anticipata in a01)
$[r, s) := \{t \in \mathbb{R} \mid r \leq t < s\}$
$(r, s] := \{t \in \mathbb{R} \mid r < t \leq s\}$
$(r, s) := \{t \in \mathbb{R} \mid r < t < s\}$

Si dice **ampiezza degli intervalli reali** il reale nonnegativo $s - r$.

Si definiscono inoltre i seguenti**intervalli reali illimitati**

$(s, +\infty) := \{t \in \mathbb{R} \mid s < t\}$
$[s, +\infty) := \{t \in \mathbb{R} \mid s \leq t\}$
$(-\infty, r) := \{t \in \mathbb{R} \mid t < r\}$
$[-\infty, r) := \{t \in \mathbb{R} \mid t \leq r\}$

B42c.05 Per ogni $y \in \mathbb{R}_{nz}$ e ogni $x \in \mathbb{R}$ useremo anche le scritture

$$1/y := \frac{1}{y} := y^{-1} \qquad \text{e} \qquad x/y := \frac{x}{y} := x \cdot \frac{1}{y} = x \cdot y^{-1} \ .$$

Si definisce **valore assoluto del reale** r e si denota con $|r|$ il numero reale preso uguale ad r sse $r \geq 0$, preso uguale a $-r$ sse $r < 0$.

Talora sono usate anche le notazioni $r^- := \dfrac{|r| - r}{2}$ e $r^+ := \dfrac{|r| + r}{2}$; per esse evidentemente

$r \geq 0 \iff r^- = 0 \ , \ r^+ = r \quad , \quad r \leq 0 \iff r^- = -r \ , \ r^+ = 0 \quad , \quad r = r^+ - r^- \quad , \quad |r| = r^- + r^+ \ .$

(1) Prop.: $\forall a \in \mathbb{R}_{0+} \ : \ |r| \leq a \iff -a \leq r \leq a \quad , \quad |r| < a \iff -a < r < a$ ∎

(2) Prop.: $\forall r, s \in \mathbb{R} \ : \ (a) : \ |r + s| \ \leq \ |r| + |s| \quad , \quad (b) : \ \Big|\, |r| - |s| \,\Big| \ \leq \ |r - s|.$

Dim.: La (a), quando r ed s sono entrambi positivi discende direttamente dalla definizione di valore assoluto e da b03(1); se r ed s sono entrambi negativi si riconduce al caso precedente.
Nel caso sia $r \leq 0 \leq s$ valgono le disuguaglianze

$$r + s \leq s \leq |r| + s = |r| + |s| \ \text{ e } \ r + s \geq r \geq r - |s| = -|r| - |s| \ .$$

Da queste si ricavano $|r| = |s + (r - s)| \leq |s| + |r - s|$ e $|s| = |r + (s - r)| \leq |r| + |s - r|$.
Queste ultime implicano $-|r - s| \ \leq \ |r| - |s| \ \leq \ |r - s|$, come si voleva.
Considerazioni simili se $s \leq 0 \leq r$ ∎

(3) Prop.: Per qualsiasi intero positivo n e per $r_1, ..., r_n \in \mathbb{R} \ : \ |r_1 + r_2 + \cdots + r_n| \leq |r_1| + |r_2| + \cdots + |r_n|$

Dim.: Si applica più volte (2)(a) ∎

B42c.06 **(1) Prop.:** Sia $t \in \mathbb{R}_{0+}$; $r \leq s \implies r\,t \leq s\,t$.

Dim.: Per b03(3) $r \leq s$ implica $0 \leq s - r$ e quindi, grazie alla $\ulcorner 0 \leq t, u \implies 0 \leq t\,u \urcorner$ abbiamo $0 \leq (s - r)\,t = s\,t - r\,t$, cioè l'asserto ∎

(2) Prop.: Sia $t \in \mathbb{R}_+$; $r < s \implies r\,t < s\,t$ ∎

(3) Prop.: $r \leq 0 \ \land \ s \geq 0 \implies r\,s \leq 0$ ∎

(4) Prop.: $r \leq 0 \ \land \ s \leq 0 \implies r\,s \geq 0$ ∎

(5) Prop.: $r < 0 \ \land \ s > 0 \implies r\,s < 0$ ∎

(6) Prop.: $r < 0 \ \land \ s < 0 \implies r\,s > 0$ ∎

(7) Prop.: $\forall r \in \mathbb{R}_{nz} : \ r^2 > 0$ ∎

(8) Prop.: $\forall r, s \in \mathbb{R} : \ |r \cdot s| = |r| \cdot |s|$ ∎

B42c.07 **(1) Prop.:** $r > 0 \implies r^{-1} > 0$ ∎

(2) Prop.: $\forall t \in \mathbb{R}_+ \ : \ r \leq s \iff r\,t \leq s\,t$ ∎

(3) Prop.: $0 < r < s \iff 0 < s^{-1} < r^{-1} \iff \forall n \in \mathbb{P} : \ 0 < r^n < s^n$.

(4) Prop.: Se $r < s$ si ha $r < \frac{r+s}{2} < s$

Dim.: Da $s - r > 0$ e (2) segue che $\frac{r+s}{2} > 0$ e quindi l'asserto ▮

(5) Coroll.: Ogni intervallo aperto non è vuoto ▮

(6) Prop.: Siano $I_1, ..., I_n$ n intervalli aperti mutuamente disgiunti, cioè tali che $h \neq k \Longrightarrow I_h \cap I_k = \emptyset$; sia inoltre J un intervallo che contiene $I_1 \cup I_2 \cup \cdots \cup I_n$. Per le ampiezze di questi intervalli si ha

$$|I_1| + |I_2| + \cdots + |I_n| \leq |J| \text{ ▮}$$

B42c.08 I numeri reali 0 e 1 si possono identificare con gli interi forniti dagli stessi segni; i numeri reali della forma $n \cdot 1 := \overbrace{1 + 1 + \cdots + 1}^{n \text{ volte}}$ si possono identificare con gli interi positivi n ed e i corrispondenti opposti con i numeri interi negativi.

Si può quindi dire con un veniale abuso di linguaggio che l'insieme dei numeri interi è un sottoinsieme dell'insieme dei reali.

I numeri reali della forma $\pm\frac{n}{d}$ con $n \in \mathbb{N}$ e $d \in \mathbb{P}$ si possono identificare con i numeri razionali.
Si può quindi dire con lieve abuso di linguaggio che l'insieme dei numeri razionali è un sottoinsieme dell'insieme dei reali.

Possiamo quindi scrivere $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

B42c.09 **(1) Prop.:** Ogni intervallo aperto di $\mathbb{R}$ non ridotto al vuoto contiene un numero razionale.

Dim.: Consideriamo l'intervallo aperto (a,b) e sia $w := b - a > 0$ la sua ampiezza. Per [Re 4] si trova un intero positivo $n > \frac{1}{w}$ e per [Re 5] $\frac{1}{n} < w$; in parole povere $\frac{1}{n}$ determina un "modo di saltare" sulla retta reale che se viene praticato da un qualche oggetto mobile che intende passare dalla sinistra alla destra dell'intervallo dato non può evitare di toccarlo almeno in un punto.

Occorre distinguere il caso $0 < b$ dal caso $b \leq 0$. Nel caso sia $0 < b$ [Re 4] garantisce che si trova un intero positivo k tale che $b \leq \frac{k}{n}$; denotiamo con h il minimo di questi valori interi k.

Dal punto razionale $\frac{k}{n}$ della retta reale, arretrando di un passo $\frac{1}{n}$ si giunge nel punto razionale $\frac{h-1}{n}$ che deve trovarsi alla sinistra di b per definizione di h e deve trovarsi alla destra di a perché in caso contrario sarebbe $b - a = w \leq \frac{1}{n}$. Abbiamo quindi trovato un definito numero razionale appartenente all'insieme dei punti opposti $(a,b) \cap \mathbb{Q}$ che denotiamo con $ratint(a, b)$.
Nel caso $b \leq 0$ si considera l'intervallo perto $(-b, -a)$ avente l'estremo superiore positivo e procedendo come sopra si trova il suo punto razionale interno esprimibile come $ratint(-b, -a)$; il suo numero opposto $-ratint(-b, -a)$ deve appartenere all'intervallo degli opposti degli elementi di $(-b, -a)$, cioè $-ratint(-b, -a) \in ((a,b) \cap \mathbb{R})$; questo è il punto richiesto ▮

(2) Prop.: Ogni intervallo aperto di $\mathbb{R}$ contiene un insieme infinito di numeri razionali.

Dim.: Il procedimento che porta dall'intervallo aperto (a,b) al razionale $ratint(a, b)$, che ora chiamiamo b_1, si può reiterare illimitatamente per gli intervalli (a, b_{j+1}) con $b_{j+1} := ratint(a, b_j)$ per $j = 1, 2, 3, ...$; Questi b_j costituiscono la successione di razionali richiesta ▮

Evidentemente la precedente successione non è unica, in quanto ad ogni passo la scelta della riduzione dell'intervallo è duplice: per ridurre (c, d) si potrebbe scegliere sia $(c, ratint(c, d))$ che $(ratint(c, d), d)$.

B42c.10 **Teorema** L'insieme dei numeri reali non è numerabile.

Dim.: L'asserto si ottiene con una tipica dimostrazione per assurdo. Si suppone di disporre di una biiezione $\beta \in \lceil \mathbb{P} \triangleleft\!\!\longrightarrow\!\!\triangleright \mathbb{R} \rceil$ e con essa si costruisce una successione di numeri reali che conduce a contraddire alcune conseguenze degli assiomi per l'insieme $\mathbb{R}$.

Definiamo iterativamente una sottosequenza crescente di interi naturali $\langle s_0, s_1, s_2, ... \rangle$ con il seguente procedimento. Poniamo $s_0 := 0$ e per s_1 assumiamo il minimo valore n per il quale $\beta(n) > \beta(0)$.

Dato che $\beta(s_0) < \beta(s_1)$ e l'intervallo aperto $(\beta(s_0), \beta(s_1))$ contiene infiniti numeri, possiamo porre $s_2 := \min\{k \;\rceil\!\rceil\; \beta(s_0) < \beta(k) < \beta(s_1)\}$.
Per analogo motivo possiamo definire $s_3 := \min\{k \;\rceil\!\rceil\; \beta(s_2) < \beta(k) < \beta(s_1)\}$.

A questo punto si possono enunciare le catene di disuguaglianze $s_0 < s_1 < s_2 < s_3$ e $\beta(s_0) < \beta(s_2) < \beta(s_3) < \beta(s_1)$.
Come dal primo intervallo $[\beta(s_0), \beta(s_1)]$ si è ottenuto il secondo $[\beta(s_2), \beta(s_3)]$, così dal secondo se ne può costruire un terzo e così via.
Quando si dispone dell'intervallo $[\beta(s_{2m-2}), \beta(s_{2m-1})]$ si definiscono $s_{2m} := \min\{k \;\rceil\!\rceil\; \beta(s_{2m-2}) < \beta(k) < \beta(s_{2m-1})\}$ e $s_{2m+1} := \min\{k \;\rceil\!\rceil\; \beta(s_{2m}) < \beta(k) < \beta(s_{2m-1})\}$.

Si giunge quindi a individuare la `saqnic` $\langle m = 0, 1, 2, ... :| \; [\beta(s_{2m}), \beta(s_{2m+1})] \rangle$.

Per l'assioma [Re 5] esiste un numero reale r contenuto in tutti questi intervalli chiusi; tale numero deve essere diverso da tutte le estremità $\beta(s_n)$ poiché entrambe le estremità di ciascun intervallo non appartengono all'intervallo successivo. Per la biiezione ipotizzata esiste un intero h tale che $r = \beta(h)$; denotiamo con n il massimo intero tale che $s_n \leq h$ e osserviamo che $h < s_{n+1}$.

Se n è pari, scrivendo $n = 2m$ si ottiene la relazione $\beta(s_{2m}) < \beta(h) < \beta(s_{2m+1}) < \beta(s_{2m-1})$, ma questa contraddice la definizione di s_{2m+1}.
Se invece n è dispari, scrivendo $n = 2m + 1$ si ha la relazione $\beta(s_{2m}) < \beta(s_{2m+2}) < \beta(h) < \beta(s_{2m+1})$, ma questa contraddice la definizione di s_{2m+1}.
L'esistenza di una biiezione β è quindi impossibile ▮

B42c.11 **Teorema** L'insieme $\mathbb{R}$ non si può porre in biiezione con gli insiemi numerabili, mentre contiene insiemi numerabili come $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}_{\mathsf{a}}$ ed $\mathbb{R}_{\mathsf{c}}$ ▮

È quindi lecito affermare che $\mathbb{R}$ è un **insieme più che numerabile**.

Alla classe degli insiemi che si possono porre in biiezione con $\mathbb{R}$ si attribuisce il cosiddetto **cardinale del continuo** denotata con il simbolo $\aleph_1$, da leggere "alef con 1".

B42c.12 **(1) Prop.**: Consideriamo un insieme $\boldsymbol{R}$ avente cardinale $\aleph_1$; per ogni $\boldsymbol{S}$ sottoinsieme numerabile di $\boldsymbol{R}$ il suo complementare $\overline{\boldsymbol{S}} := \boldsymbol{R} \setminus \boldsymbol{S}$ ha il cardinale $\aleph_1$.

Dim.: Mettendo in evidenza i suoi elementi si può scrivere $\boldsymbol{S} = \{s_0, s_1, s_2, ..., s_n, ...\}$ e se fosse numerabile $\overline{\boldsymbol{S}}$ mettendo in evidenza i suoi elementi si potrebbe scrivere $\overline{\boldsymbol{S}} = \{\overline{s}_0, \overline{s}_1, \overline{s}_2, ..., \overline{s}_n, ...\}$; si potrebbe quindi ricavare una successione degli elementi di $\mathbb{R}$ eliminando le ripetizioni dalla successione $\langle s_0, \overline{s}_0, s_1, \overline{s}_1, s_2, \overline{s}_2, ..., s_n, \overline{s}_n, ... \rangle$, e quindi $\boldsymbol{R}$ sarebbe numerabile ▮

(2) Prop.: Consideriamo un insieme $\boldsymbol{R}$ avente cardinale $\aleph_1$; per ogni $\boldsymbol{F}$ sottoinsieme finito di $\boldsymbol{R}$ il suo complementare $\overline{\boldsymbol{F}} := \boldsymbol{R} \setminus \boldsymbol{S}$ ha il cardinale $\aleph_1$.

Dim.: Si può ampliare $\boldsymbol{F}$ con un suo sovrainsieme numerabile $\boldsymbol{G}$ sottoinsieme di $\boldsymbol{R}$ e quindi se fosse $\boldsymbol{R} \setminus \boldsymbol{F}$ numerabile avrebbe cardinale $\aleph_1$ anche il suo sottoinsieme $\boldsymbol{R} \setminus \boldsymbol{G}$, in contrasto con (1) ▮

(3) Coroll.: Hanno il cardinale $\aleph_1$ anche i seguenti sottoinsiemi di $\mathbb{R}$, elencati in ordine di estesione crescente:

l'insieme dei reali non costruibili $\mathbb{R} \setminus \mathbb{R}_{\mathsf{c}}$,

insieme dei reali nonalgebrici $\mathbb{R} \setminus \mathbb{R}_{\mathsf{a}}$,

insieme dei numeri irrazionali $\mathbb{R} \setminus \mathbb{Q}$,

insieme dei numeri reali non interi $\mathbb{R} \setminus \mathbb{Z}$,

insieme cofinito di numeri reali $\mathbb{R} \setminus \boldsymbol{F}$ per ogni $\boldsymbol{F}$ insieme finito di reali.

Per i numeri reali che non sono reali costruibili si può utilizzare anche il termine **numeri reali non esemplificabili**, piuttosto significativo.
Infatti ciascuno di essi non può essere individuato costruttivamente, in quanto se lo fosse si avrebbe una procedura che lo fornisce e questo lo farebbe collocare in $\mathbb{R}_{\mathsf{c}}$.

B42 d. notazioni posizionali e approssimazioni dei numeri reali

B42d.01 Ad una successione di bits $\mathsf{b} = \langle b_0, b_1, b_2, ...\rangle$, dove $\forall i \in \mathbb{P} \,\colon\, b_i = 0, 1$, è associata la serie di numeri razionali individuata dalla notazione binaria

(1) $$0.b_1\, b_2\, b_3 \ldots \;:=\; \sum_{i=1}^{+\infty} \frac{b_i}{2^i} \;.$$

Si tratta di una serie convergente di razionali positivi e quindi a essa si può associare una successione `srnic` e quindi un numero reale.

Si osserva che la scrittura binaria $0.1\,1\,1\ldots$ porta allo stesso numero 1 associato alla scrittura $1.0\,0\,0\ldots_2$ e che una scrittura della forma $0.b_1\,b_2\ldots b_{s-1}0\,1\,1\,1\ldots_2$ per $s \in \mathbb{P}$ porta allo stesso numero fornito dalla $0.b_1\,b_2\ldots b_{s-1}\,1\,0\,0\,0\ldots_2$, scrittura che da un certo punto in poi presenta solo degli zeri e che rappresenta un numero razionale multiplo di $\dfrac{1}{2^{s-1}}$.

Denotiamo con $[0,1)_{bin}$ l'insieme delle scritture $0.b_1\,b_2\,b_3\ldots_2$ a esclusione di quelle che da un certo punto in poi presentano solo bits uguali ad 1.
Diciamo **numero reale binario** una entità numerica esprimibile come somma di un intero e di un numero di $[0,1)_{bin}$; l'insieme di tali entità lo denotiamo con $\mathbb{R}_{bin}$.

Non è difficile rendersi conto che ogni reale costruibile r si può identificare con un numero reale binario. Infatti per ogni $s \in \mathbb{P}$ (intuitivamente pensato arbitrariamente grande) una procedura in grado di approssimare quanto si vuole un $q \in \mathbb{R}_{\mathsf{C}}$ è in grado di individuare le cifre binarie della scrittura della for $c_h\,c_{h-1}\ldots c_0\,.\,b_1\,b_2\ldots b_s\,b_{s+1}$ che individui un razionale $\overline{q}$ che approssimi q tanto da che si possa affermare $|q-\overline{q}| < 2^{-s}$, ossia con uno scarto piccolo quanto si vuole.

B42d.02 L'insieme $[0,1)_{bin}$ è costituito dai numeri reali maggiori o uguali a 0 e minori di 1.

(1) Lemma: L'insieme $[0,1)_{bin}$ ha il cardinale di $\mathfrak{P}(\mathbb{P})$ ▮

(2) Lemma: L'insieme dei reali binari ha cardinale $\aleph_1$.

Dim.: La trasformazione $\lceil\, x \in (0,1) \mapsto \dfrac{x-1/2}{x(1-x)} \,\rceil \,\dot\cup\, \lceil\, 0 \mapsto 0 \,\rceil$ pone in biiezione l'intervallo $[0,1)$ con l'intero $\mathbb{R}$; quindi questo insieme ha il cardinale del continuo ▮

La trasformazione precedente si serve solo di poche semplici operazioni razionali ma non è geometricamente intuitiva.
Una trasformazione continua e geometricamente giustificabile, ma che richiede operazioni infinitesimali, è la

$$\lceil\, x \in (0,1) \mapsto \tan \pi \left(x - \frac{1}{2}\right) \,\rceil \;.$$

B42d.03 Il cardinale di $\mathfrak{P}(\mathbb{P})$, $\aleph_1$, è superiore al cardinale del numerabile $\aleph_0$ in virtù del teorema di Cantor.

Il termine cardinale del continuo è in accordo con il fatto che segue.

Teorema L'insieme dei reali costruibili è in biiezione con un sottoinsieme proprio dell'insieme dei numeri reali binari.

Dim.: I reali costruibili hanno il cardinale del numerabile, in quanto sono tutti esprimibili con procedure esprimibili con un linguaggio numerabile; i reali hanno cardinale superiore ▮

B42d.04 I numeri in $\mathbb{R}_{bin} \setminus \mathbb{R}_{\mathsf{C}}$ non possono essere concretamente utilizzati in calcoli specifici.
Essi servono invece, in quanto $\mathbb{R}$ si rivela un ambiente assai vantaggioso per ogni presentazione formalmente accurata dei risultati degli studi delle funzioni tra insiemi numerici.

Dato che l'insieme dei reali costruibili per definizione comprende tutti i numeri reali utilizzabili nelle pratiche computazionali, si deve dire, a prima vista paradossalmente, che i numeri reali sono caratterizzati dall'includere i numeri reali non esemplificabili, oggetti completamente inutilizzabili nelle elaborazioni specifiche e anche nelle argomentazioni su oggetti riconducibili a numeri e a funzioni specifiche.

Si trova che l'insieme dei numeri introdotti con le classi della equivalenza-lim si può porre in biiezione con l'insieme dei numeri introdotti con le sezioni del campo razionale.
Queste ultime consentono di argomentare un po' più speditamente delle `saqnic`, ma si servono di entità (le sezioni come coppie di totalità di numeri razionali con date proprietà) che non si possono ricondurre direttamente ad attività costruttive come quelle che intervengono negli studi che richiedono indagini numeriche.

B42 e. estremo superiore ed estremo inferiore

B42e.01 Consideriamo un insieme nonvuoto di numeri reali $S \subseteq_{ne} \mathbb{R}$.
Si dice **minorante dell'insieme di reali** S ogni reale m tale che $\forall r \in S \,:\, m \leq r$. Per dualità-UD si dice **maggiorante** di S ogni reale M tale che $\forall r \in S \,:\, r \leq M$.

Denotiamo con $\mathsf{Mnrnt}(S)$ l'insieme dei minoranti di S e con $\mathsf{Mjrnt}(S)$ l'insieme dei maggioranti di S.

Evidentemente per ogni $r, s \in \mathbb{R}$ con $r < s$ abbiamo

$$\mathsf{Mnrnt}(r) = \mathsf{Mnrnt}[r,s] = \mathsf{Mnrnt}[r,s) = \mathsf{Mnrnt}(r,s) = (-\infty, r) \quad ;$$
$$\mathsf{Mjrnt}(s) = \mathsf{Mjrnt}[r,s] = \mathsf{Mjrnt}(r,s] = \mathsf{Mjrnt}(r,s) = (s, +\infty] \ .$$

È anche evidente che ogni minorante di un minorante di un insieme di reali S è vuoto e che ogni maggiorante di un maggiorante di un tale S è vuoto.
Questo equivale ad affermare che Mnrnt e Mjrnt sono funzioni di insieme nilpotenti, ossia che

$$\forall S \subseteq \mathbb{R} \quad : \quad \mathsf{Mnrnt}(\mathsf{Mnrnt}(S) = \emptyset \quad , \quad \mathsf{Mjrnt}(\mathsf{Mjrnt}(S) = \emptyset \ .$$

L'insieme di reali S si dice **insieme limitato superiormente** o insieme maggiorato sse possiede un maggiorante; in tal caso possiede infiniti maggioranti.
Dualmente-UD S si dice **insieme limitato inferiormente** o insieme minorato sse possiede un minorante; in tal caso possiede infiniti minoranti.
Inoltre S si dice **insieme limitato** sse è limitato superiormente e inferiormente, cioè sse possiede maggioranti e minoranti.

Evidentemente ogni intervallo di ampiezza finita è limitato e ogni insieme finito di reali è limitato.
Gli insiemi $\mathbb{N}$ e $\mathbb{P}$ sono limitati inferiormente ma illimitati superiormente; $\mathbb{Z}$ non è limitato né inferiormente, né superiormente.

Inoltre un sottoinsieme S di $\mathbb{R}$ è limitato sse esiste un intero M tale che $\forall r \in S \,:\, |r| < M$.

B42e.02 **Teorema** Per ogni S sottoinsieme di $\mathbb{R}$ limitato superiormente l'insieme dei maggioranti possiede l'elemento minimo.

Dim.: Poniamo $\mathbf{M} := \mathsf{Mjrnt}(S)$, denotiamo con r un elemento di S e con M un elemento di $\mathbf{M}$; inoltre consideriamo un arbitrario intero positivo n.
b01
[Re 4] garantisce che esiste un m tale che $M \leq r + m\,2^{-n}$.

Denotiamo con p_n il minimo valore di m per il quale $r + m2^{-n} \in \mathbf{M}$ e introduciamo l'insieme numerico $I_n := [a + (p_n - 1)\,2^{-n} \ , \ a + p_n\,2^{-n}]$; si constata che $S \cap I_n \neq \emptyset$.
Dato che $p_n\,2^{-n} = 2\,p_n\,2^{-(n+1)}$, deve essere $p_{n+1} = 2\,p_n$ oppure $p_{n+1} = 2\,p_n - 1$; di conseguenza $I_{n+1} \subset I_n$.
La successione degli I_n costituisce una `srni` e per b01[Re 5] la intersezione di tali intervalli è un insieme nonvuoto che denotiamo con $U := \bigcap_{n=1}^{+\infty} I_n$.

Se U contenesse due elementi diversi α e β l'intervallo $[\alpha, \beta]$ sarebbe contenuto nell'intervallo I_n di ampiezza 2^{-n} per n qualsiasi, cosa assurda in quanto implicherebbe $1 \geq 2^n\,(\beta - \alpha)$ per ogni n. Di conseguenza U contiene un solo numero reale che denotiamo con u.
Questo numero è maggiorante di S, in quanto in caso contrario si avrebbe un elemento di $S \ {}^{\searrow} s > u$ e dato che u appartiene a tutti gli I_n, varrebbe la relazione $r + p_n\,2^{-n} < s$, incompatibile con la definizione di p_n.

Inoltre per nessuno degli $M \in \mathsf{M}$ può essere $M < u$, in quanto tale disuguaglianza implicherebbe l'esistenza di un intero positivo n tale che $2^{-n} < u - M$ e la relazione $u \in I_n$ avrebbe come conseguenza $r + (p_n - 1)2^{-n} > u$, relazione anch'essa incompatibile con la definizione di p_n.
Si conclude quindi che il numero reale u è il minimo elemento di M ∎

B42e.03 **(1) Coroll.**: Per ogni T sottoinsieme di $\mathbb{R}$ limitato inferiormente l'insieme dei minoranti possiede l'elemento massimo.

Dim.: Basta applicare il teorema precedente all'insieme dei numeri opposti degli elementi di T, cioè ad $S := \{r \in S :| \ -r\}$ ∎

Come il corollario precedente si può ricavare dal teorema e02, molte altre costruzioni (definizioni e proprietà) riguardanti le caratteristiche di ordinamento dei numeri reali si possono considerare in coppie nelle quali ciascuna delle due costruzioni si ottiene dall'altra applicando la permutazione cambiamento di segno $\lceil r \in \mathbb{R} \mapsto \ -r \rceil$; questa è la riflessione di $\mathbb{R}$ rispetto allo 0 e la denoteremo con $ReflR_0$.

In questi casi si parla di **duetti di costruzioni riflesse**, ovvero **invarianti per riflessione** $ReflR_0$. Il collegamento tra i membri di queste coppie costituisce un caso particolare della dualità-LR.

Tra le coppie di costruzioni in conseguenza della riflessione $ReflR_0$ vengono a scambiarsi vi sono: i minoranti con i maggioranti, limitatezza inferiore e limitatezza superiore, illimitatezza inferiore e illimitatezza superiore, elemento minimo ed elemento massimo.
Vanno notate anche le costruzioni che in conseguenza della riflessione $ReflR_0$ rimangono invariate, entità che chiamiamo **costruzioni autoriflesse** e che costituiscono esempi delle cosiddette **costruzioni autoduali**. Per ora abbiamo incontrato solo la proprietà di limitatezza (inferiore e superiore) e la proprietà opposta di illimitatezza (inferiore e superiore).

B42e.04 Il minimo dei maggioranti di un insieme S di numeri reali viene detto **estremo superiore** o **supremo** di S e si denota con $\sup(S)$.
Il massimo dei minoranti di un insieme S di numeri reali viene detto **estremo inferiore** o **infimo** di S e si denota con $\inf(S)$.
Ogni L sottoinsieme nonvuoto di $\mathbb{R}$ limitato possiede entrambi gli estremi ed evidentemente $\inf(L) \leq \sup(L)$.
È evidente anche che estremo inferiore ed estremo superiore sono costruzioni duali-LR.

(1) Prop.: Sia S un insieme di reali limitato superiormente.

$$u = \sup(S) \iff u \in \mathsf{Mjrnt}(S) \ \wedge \ \forall n \in \mathbb{P} \ \vdots \ S \ni s_n \ \rrbracket \ u - \frac{1}{n} < s_n \leq u \ .$$

Dim.: Cfr. sopra ∎

(2) Prop.: Sia S un insieme di reali limitato inferiormente.

$$u = \inf(S) \iff u \in \mathsf{Mnrnt}(S) \ \wedge \ \forall n \in \mathbb{P} \ \vdots \ S \ni s_n \ \rrbracket \ u + \frac{1}{n} > s_n \geq u \ .$$

Dim.: Duale-LR della (1) ∎

B42e.05 **(1) Prop.**: Siano S un insieme di reali limitato superiormente e $T \subseteq S$; anche T è limitato superiormente e $\sup(T) \leq \sup(S)$ ∎

(2) Prop.: Siano S un insieme di reali limitato inferiormente e $T \subseteq S$; anche T è limitato inferiormente ed $\inf(S) \leq \sup(T)$ ∎

(3) Prop.: Consideriamo una famiglia di sottoinsiemi non vuoti di $\mathbb{R}$ $^{\searrow}$ $\{\mu \in M :| \ S_\mu\}$; inoltre poniamo $T := \bigcup_{\mu \in M} S_\mu\}$ e $U := \{\mu \in M :| \ \sup M_\mu\}$. L'unione T è superiormente limitato sse lo è U e in tal caso $\sup T = \sup U$.

Dim.: Basta considerare che $\mathsf{Mjrnt}(T) = \mathsf{Mjrnt}(U)$ ▮

(4) Prop.: Consideriamo una famiglia di sottoinsiemi non vuoti di $\mathbb{R}$ $^{\searrow}$ $\{\mu \in M :| S_\mu\}$; siano inoltre $T := \bigcup_{\mu \in M} S_\mu\}$ e $I := \{\mu \in M :| \inf(M_\mu)\}$.
L'unione T è inferiormente limitato sse lo è U e in tal caso $\inf T = \inf U$.

Dim.: Basta considerare che che $\mathsf{Mnrnt}(T) = \mathsf{Mnrnt}(U)$, oppure che si tratta dell'enunciato duale-LR di (3) ▮

B42e.06 Consideriamo una funzione f del genere $\lceil D \longmapsto \mathbb{R} \rceil$ con $D \subseteq_{ne} \mathbb{R}$. Essa si dice **funzione limitata superiormente** sse $\mathsf{cod}(f)$ è limitato superiormente.
Dualmente-UD si dice **limitata inferiormente** sse $\mathsf{cod}(f)$ è limitato inferiormente.

Se $\mathsf{cod}(f)$ è limitato superiormente si dice **estremo superiore della funzione** e si scrive

$$\sup_{x \in D} f(x) \ := \ \sup(\mathsf{cod}(f)) \ .$$

Dualmente-UD se $\mathsf{cod}(f)$ è limitato inferiormente si dice **estremo inferiore della funzione** e si scrive

$$\inf_{x \in D} f(x) \ := \ \inf(\mathsf{cod}(f)) \ .$$

B42e.07 **(1) Prop.**: Consideriamo la funzione $f(x) \in \lceil D \longmapsto \mathbb{R} \rceil$.
(a) Se $f(x)$ è limitata superiormente, allora la $-f(x)$ è limitata inferiormente e

$$\inf_{x \in D}(-f(x)) \ = \ -\sup_{x \in D} f(x) \ ▮$$

(b)Se $f(x)$ è limitata inferiormente, allora la $-f(x)$ è limitata superiormente e

$$\sup_{x \in D}(-f(x)) \ = \ -\inf_{x \in D} f(x) \ ▮$$

(2) Prop.: Consideriamo $D_1, D_2 \subseteq_{ne} \mathbb{R}$ e una funzione f del genere $\lceil D_1 \times D_2 \longmapsto \mathbb{R} \rceil$.
(a) Se f è limitata superiormente, allora

$$\sup_{\langle x_1, x_2 \rangle \in D_1 \times D_2} \ = \ \sup_{x_1 \in D_1} (\sup_{x_2 \in D_2} (f(x_1, x_2)) \ = \ \sup_{x_2 \in D_2} (\sup_{x_1 \in D_1} (f(x_1, x_2)) \ .$$

(b) Se f è limitata inferiormente, allora

$$\inf_{\langle x_1, x_2 \rangle \in D_1 \times D_2} \ = \ \inf_{x_1 \in D_1} (\inf_{x_2 \in D_2} (f(x_1, x_2)) \ = \ \inf_{x_2 \in D_2} (\inf_{x_1 \in D_1} (f(x_1, x_2)) \ .$$

Dim.: (a) L'insieme $\mathsf{cod}(f)$ si può esprimere come $\displaystyle\bigcup_{x_1 \in D_1} f(x_1, D_2)$ e quindi basta applicare e05(3) ▮

(b) Enunciato duale-UD di (a) ▮

(3) Prop.: Consideriamo $f, g \in \lceil D \longmapsto \mathbb{R} \rceil$ tali che $\forall x \in D : f(x) \leq g(x)$.

(a) Se $g(x)$ è limitata superiormente in D lo è anche $f(x)$ e si ha

$$\sup_{x \in D}(f(x)) \leq \sup_{x \in D}(g(x)) \ .$$

(b) Se $f(x)$ è limitata inferiormente in D lo è anche $g(x)$ e si ha

$$\inf_{x \in D}(f(x)) \leq \inf_{x \in D}(g(x)) \ .$$

Dim.: Scende direttamente dalle definizioni ▮

B42e.08 **(1) Prop.**: Consideriamo $D \subseteq_{ne} \mathbb{R}$ e le funzioni $f(x), g(x) \in \lceil D \longmapsto \mathbb{R} \rceil$.

(a) Se $f(x)$ e $g(x)$ sono entrambe limitate superiormente, allora lo è anche la loro somma

$f+g := \lceil x \in D \mapsto f(x)+g(x) \rceil$ e $\sup_{x\in D}[f(x)+g(x)] \leq \sup_{x\in D} f(x) + \sup_{x\in D} g(x)$.

(b) Se inoltre $g(x)$ è limitata inferiormente, allora
$\sup_{x\in D} f(x) + \inf_{x\in D} g(x) \leq \sup_{x\in D}(f(x)+g(x))$.

(c) Se $f(x)$ e $g(x)$ sono entrambe limitate inferiormente, allora lo è anche la loro somma $f+g$ e
$\inf_{x\in D}(f(x)+g(x)) \geq \inf_{x\in D} f(x) + \inf_{x\in D} g(x)$.

(d) Se inoltre $g(x)$ è limitata superiormente, allora
$\inf_{x\in D} f(x) + \sup_{x\in D} g(x) \geq \inf_{x\in D}(f(x)+g(x))$.

Dim.: Poniamo $F := \sup_{x\in D} f(x)$ e $G := \sup_{x\in D} g(x)$; di conseguenza $\forall x \in D \;\colon\; f(x) \leq F \wedge g(x) \leq G$ e quindi $\forall x \in D \;\colon\; f(x)+g(x) \leq F+G$ e dunque (a).
Se inoltre esiste $I := \inf_{x\in D} g(x)$, allora, posto $J := \sup_{x\in D}(f(x)+g(x))$, si ha $\forall x \in D \;\colon\; f(x)+I \leq J$ e quindi $\forall x \in D \;\colon\; f(x) \leq J-I$ e dunque $F \leq J-I$, ovvero $F+I \leq J$, ossia la tesi di (b).
Per concludere gli enunciati (c) e (d) si ottengono per dualità-UD di (a) e (b) ▮

B42e.09 Consideriamo $D \subseteq_{ne} \mathbb{R}$ e la funzione $f(x) \in \lceil D \longmapsto \mathbb{R} \rceil$.

(1) Prop.: Se $f(x)$ è limitata superiormente, allora $\forall c \in \mathbb{R} \;\colon\; \sup_{x\in D}(f(x)+c) = \sup_{x\in D} f(x) + c$.

Dim.: Si può derivare da e08 nel caso $g(x) = \lceil x \in D \mapsto c \rceil$ ▮

(2) Prop.: Se $f(x)$ è limitata inferiormente, allora $\forall c \in \mathbb{R} \;\colon\; \inf_{x\in D}(f(x)+c) = \inf_{x\in D} f(x) + c$.

Dim.: Proprietà duale-UD della (1) ▮

Consideriamo $D_1, D_2 \subseteq_{ne} \mathbb{R}$, le funzioni $f_1(x) \in \{D_1 \longmapsto \mathbb{R} \rceil$ e $f_2(x) \in \lceil D_2 \longmapsto \mathbb{R} \rceil$ e la loro composizione

$$S(\mathsf{x}) := \left\lceil \langle x_1, x_2 \rangle \in D_1 \times D_2 \mapsto f_1(x_1) + f_2(x_2) \right\rceil .$$

(3) Prop.: Se $f_1(x)$ ed $f_2(x)$ sono funzioni limitate superiormente, allora lo è anche la funzione $S(\mathsf{x})$ e

$$\sup_{\langle x_1,x_2 \rangle \in D_1 \times D_2} (f_1(x_1) + f_2(x_2)) = \sup_{x_1 \in D_1} f_1(x_1) + \sup_{x_2 \in D_2} f_2(x_2) .$$

Dim.: Discende da e07(2) e da (2) ▮

(4) Prop.: Se $f_1(x)$ ed $f_2(x)$ sono funzioni limitate inferiormente, allora lo è anche la funzione $S(\mathsf{x})$ e

$$\inf_{\langle x_1,x_2 \rangle \in D_1 \times D_2} (f_1(x) + f_2(x)) = \inf_{x_1 \in D_1} f_1(x_1) + \inf_{x_2 \in D_2} f_2(x_2) .$$

Dim.: Proprietà duale-UD della (3) ▮

B42 f. altre assiomatizzazioni dei numeri reali

B42f.01 I numeri reali possono essere introdotti con vari sistemi di assiomi diversi da quello presentato in b01. Qui cominciamo con il presentare una sua variante tutto sommato modesta, l'assiomatizzazione più ampiamente adottata talora chiamata assiomatizzazione sintetica la quale definisce l'insieme dei numeri reali come un **campo ordinato** per il quale vale la proprietà di completezza di Dedekind [a01].

Dell'entità individuata dall'asssiomatizzazione sintetica si possono costruire vari modelli che si dimostrano essere equivalenti; in particolare i modelli basati sulle successioni di Cauchy, sulle sezioni di Dedekind e sulle notazioni decimali o, più in generale basati sulle scritture posizionali relative a una base $B = 2, 3, ...$

B42f.02 Definiamo come **insieme dei numeri reali** la struttura algebrico-relazionale $\langle \mathbb{R}, +, \cdot, -, ^{-1}, 0, 1, \leq \rangle$ che soddisfa le richieste che seguono.

[Reo 1] $\langle \mathbb{R}, +, \cdot, -, ^{-1}, 0, 1, \rangle$ è un campo, cioè in dettaglio
- $+$ è un'operazione binaria su $\mathbb{R}$ associativa e commutativa chiamata somma;
- 0 è l'elemento neutro per la somma, cioè $\forall x \in \mathbb{R} : x + 0 = x$;
- $-$ è l'operazione di passaggio all'inverso per la somma, cioè: $\forall x \in \mathbb{R} : x + (-x) = 0$;
- $\cdot$ è un'operazione binaria su $\mathbb{R}$ associativa e commutativa chiamata prodotto;
- 1 è diverso da 0 ed è l'elemento neutro per il prodotto, cioè $\forall x \in \mathbb{R} : 1 \cdot x = x$;
- $^{-1}$ è l'operazione di passaggio all'inverso per il prodotto, ma limitatamente a $\mathbb{R}_{nz} := \mathbb{R} \setminus \{0\}$, cioè $\forall x \in \mathbb{R}_{nz} : x \cdot x^{-1} = 1$;
- il prodotto è distributivo rispetto alla somma, cioè $\forall x, y, z \in \mathbb{R} : x \cdot (y + z) = x \cdot y + x \cdot z$;

[Reo 2] $\langle \mathbb{R}, \leq 4 \rangle$ è un insieme totalmente ordinato, cioè
- $\forall x \in \mathbb{R} : x \leq x$ (riflessività);
- $\forall x, y \in \mathbb{R} : x \leq y \ , \ y \leq x \Longrightarrow x = y$ (antisimmetria);
- $\forall x, y, z \in \mathbb{R} : x \leq y \ , \ y \leq z \Longrightarrow x \leq z$ (transitività);
- $\forall x, y \in \mathbb{R} : x \leq y \vee y \leq x$ (totalità dell'ordine).

[Reo 3] Le operazioni $+$ e $\cdot$ sono compatibili con l'ordine, cioè
- $\forall x, y, z \in \mathbb{R} : x \leq y \Longrightarrow x + z \leq y + z$ (mantenimento dell'ordine da parte della somma);
- $\forall x, y, z \in \mathbb{R} : 0 \leq x \leq y \ , \ 0 \leq z \Longrightarrow x \cdot y \leq y \cdot z$ (mantenimento dell'ordine da parte del prodotto);

[Reo 4] L'ordine $\leq$ è completo secondo Dedekind, ossia ogni S sottoinsieme nonvuoto di $\mathbb{R}$ limitato superiormente contiene un elemento u (suo estremo superiore) tale che per ogni v maggiorante di S si ha $u \leq v$.

B42f.03 Gli assiomi [Reo 1], [Reo 2] e [Reo 3] definiscono la struttura della specie campo ordinato; in questa specie si conoscono diverse strutture non isomorfe al campo ordinato dei numeri reali, come il campo di razionali e il campo delle funzioni razionali con coefficienti razionali.

È opportuno segnalare anche che ogni campo di classi di resti non è ordinabile.

L'assioma di completezza (4) consente invece di individuare una struttura unica a meno di isomorfismi: infatti si dimostra che tutti i modelli del sistema di assiomi [Reo 1] ∧ [Reo 2] ∧ [Reo 3] ∧ [Reo 4], cioè tutte le costruzioni di strutture che soddisfano tale sistema di enunciati portano a strutture tra loro isomorfe.
Esiste quindi essenzialmente una sola struttura di campo ordinato dei numeri reali che denotiamo con $\mathbb{R}_{Fld}$.

Si dimostra anche che questa struttura, proprio in virtù della proprietà di completezza di Dedekind, soddisfa la proprietà di Archimede.

B42f.04 Oltre alla assiomatizzazione sintetica, sono state proposte altre assiomatizzazioni dei numeri reali. Una particolarmente compatta ed elegante è stata proposta da Alfred Tarski nel 1936 [`Tarski's axiomatization of the reals` (we)].
Essa si dimostra equivalente a quella data sopra; questa dimostrazione è però piuttosto elaborata e questo ha fatto sì che la **assiomatizzazione di Tarski** sia poco diffusa.

Altre formulazioni vicine a quella di Tarski ma più semplici sono state trovate negli anni 2002-2004: queste consentono di definire i numeri reali servendosi solo dei numeri interi, senza fare ricorso diretto ai numeri razionali.

B42 g. insieme dei reali e altri insiemi più che numerabili

B42g.01 Fino alla definizione dei numeri reali costruibili abbiamo incontrato solo insiemi procedurali [B18c].
Un insieme finito può essere generato da un meccanismo realizzabile che opera attraverso una sequenza finita di passi e quindi può essere costruito e riutilizzato effettivamente.
Anche gli elementi di un insieme procedurale possono essere concretamente utilizzati, in quanto la loro generazione può essere portata avanti da procedure concretamente definibili tanto quanto si vuole, compatibilmente con le risorse di memoria e di tempo di elaborazione che sono disponibili caso per caso.
Qui per semplicità trascuriamo gli insiemi ricorsivamente enumerabili in quanto poco utilizzabili e ci limitiamo a considerare gli **insiemi contabili**, cioè gli insiemi finiti o numerabili.

Per trattare sistematicamente gli insiemi contabili si sono introdotte procedure primarie che consentono di costruire pochi insiemi fondamentali, e altre procedure (selettive, compositive, ...) che a partire da insiemi contabili noti portano ad altri insiemi contabili (ma con il rischio di condurre a insiemi ricorsivamente enumerabili non ricorsivi).

Negli insiemi contabili si possono ambientare importanti sviluppi conoscitivi ed elaborativi: questi insiemi sono gli ambienti nei quali si effettuano le attività computazionali; a livello metodologico queste sono governate da algoritmi, l'ambito matematico nei quali questi sono studiati viene chiamato `matematica discreta (wi)` e importanti teorie inquadrano quest'area, in particolare le cosiddette `teorie combinatorie (wi)`.

Vi sono però sviluppi conoscitivi matematici di importanza vitale, i quali tra l'altro sono indispensabili per i modelli fisico-matematici e quindi per lo sviluppo delle conoscenze scientifiche, tecnologiche, statistiche, economiche, ... che si servono di entità che presentano molte caratteristiche in comune con gli insiemi contabili, ma che non sono riconducibili a meccanismi realizzabili.

In questa sezione introdurremo senza indagare a fondo sulla loro natura queste entità che inizialmente chiamiamo, un po' genericamente **insiemi più che numerabili**. I numeri reali sono le prime entità di questo genere e qui faremo riferimento soprattutto a esse.

B42g.02 Si potrebbe pensare che questi insiemi non sono indispensabili per studiare le attività elaborative concrete, in quanto queste, a rigore, hanno a che fare solo con oggetti costituenti insiemi contabili.

Gli insiemi più che numerabili, in quanto non ottenibili con una effettiva costruzione finita o potenzialmente illimitata, possono essere studiati solo attraverso rappresentazioni strettamente formali.

Le loro proprietà si devono ottenere a partire da definizioni "formalmente precise ed esaurienti" e servendosi di procedimenti dimostrativi a loro volta da definire con "precisione formale" e da applicare con "meticoloso rigore formale".

Questi sviluppi si dicono costituire la **matematica assiomatico-deduttiva**.

Si riscontra che queste attività presentano aspetti che in parte sono riconducibili ad algoritmi e a costruzioni effettive, mentre in parte prescindono dalla costruibilità e si pongono in una sorta di contrapposizione con la matematica costruttiva e con l'elaborazione dei dati.

B42g.03 La matematica assiomatico-deduttiva, nel corso della storia del pensiero scientifico e dei movimenti culturali che hanno tenuto in maggior conto la razionalità, si è rivelata una disciplina molto attenta alle questioni metodologiche, notevolmente stabile nei suoi risultati specifici e nel suo assetto complessivo, assai apprezzata per i suoi molteplici contributi e stimoli alle altre discipline e per la esemplarità del suo modus operandi. Inoltre nei tempi lunghi ha saputo allargare la sua portata evitando i ripensamenti con conseguenze distruttive che si incontrano nella storia di varie discipline.

Fino alla prima parte del 1900 l'osservazione del suo rigore ha alimentato la speranza di accertare con metodi matematici la infallibilità del suo procedere e quindi la pretesa che la matematica, nel suo ambito, fosse portatrice di verità inconfutabili per l'eternità [v. in particolare C21].

Questa speranza è però risultata illusoria in seguito a risultati di incompletezza, scoperti da Goedel e si è giunti a parlare di "perdita della certezza".

La fiducia nell'affidabilità dei risultati della matematica resta molto alta e a questo contribuisce anche la determinazione con la quale molti matematici hanno indagato sui propri limiti.

Occorre anche osservare il continuo vigoroso progredire di questa disciplina che, anche se poco percepito da tanti ambienti culturali, la mantiene saldamente alla base delle attività scientifiche e tecnologiche, in buona sintonia con la meditata convinzione che vede queste ultime procedere servendosi di modelli falsificabili.

Lo studio degli insiemi più che numerabili, e quindi i procedimenti assiomatico-deduttivi, si sono imposti fin dalla stagione della grande matematica greco-ellenistica (dal VI al II secolo a.C), in seguito alle esigenze della geometria, della meccanica e di gran parte degli studi dei fenomeni naturali e tecnici che cercano risultati quantitativi che possano essere riutilizzati affidabilmente.

Gli studi assiomatico-deduttivi si sono sviluppati ottenendo risultati di grande portata e profondità che in molte occasioni sono stati determinanti e talora anche trascinanti per lo sviluppo della scienza e della tecnologia fino ai nostri giorni.

Non va tuttavia dimenticato che per affrontare molti problemi è accaduto che si procedesse, anche a lungo, con atteggiamenti euristici, in mancanza di fondamenti rigorosi e talora in presenza di scuole matematiche schierate su posizioni contrastanti.

In effetti lo sviluppo della matematica assiomatico-deduttiva ha portato a risultati che hanno permesso di individuare procedimenti costruttivi mentali e automatizzabili efficaci e di ampia applicabilità.

B42g.04 Una entità che si presenta naturalmente nello sviluppo della matematica discreta è la collezione di tutti gli insiemi costituiti da interi naturali.

In sintonia con la definizione, anche costruttiva, dei booleani degli insiemi finiti F, dei $\mathfrak{P}(F)$, questa collezione è stata chiamata **insieme dei sottoinsiemi** di $\mathbb{N}$, **insieme delle parti** di $\mathbb{N}$ o **booleano** di $\mathbb{N}$ ed è stata denotata con $\mathfrak{P}(\mathbb{N})$.

È facile rendersi conto che questa entità consente di discutere dei problemi numerici in termini più semplici e concisi, e quindi risulta naturale prenderla in seria e deinitiva considerazione.

Questa collezione si è scoperta molto vicina a quella delle sequenze binarie infinite $b_1b_2...$, cioè alla collezione di funzioni $\lceil \mathbb{N} \longmapsto \mathbb{B} \rceil$. Le suddette sequenze si è sono trovate in corrispondenza biunivoca con i numeri esprimibili in forma binaria come $0.b_1b_2..._2$, numeri compresi tra 0 e 1 i quali rivestono notevole importanza computazionale.

B42g.05 Dimostriamo ora il seguente risultato di importanza storica.

Teorema (**teorema di Cantor**)
$\mathfrak{P}(\mathbb{N})$ non può essere un insieme numerabile.

Dim.: Procedendo per assurdo, supponiamo che $\mathfrak{P}(\mathbb{N})$ sia numerabile e quindi che esista una biiezione $\beta \in \lceil \mathbb{N} \triangleleft\!\!\!\rightarrow\!\!\!\triangleright \mathfrak{P}(\mathbb{N}) \rceil$; consideriamo dunque l'insieme $C := \lceil n \in \mathbb{P} :| \; n \notin \beta(n) \rceil$ ed il suo complementare $\overline{C} := \lceil n \in \mathbb{N} :| \; n \in \beta(n) \rceil$.
Dovendo essere $C \in \mathfrak{P}(\mathbb{N})$, dovrebbe trovarsi in $\mathbb{N}$ un c tale che si abbia $C = \beta(c)$.
Ci chiediamo allora se questo intero appartiene a C o meno. Se fosse $c \in C$ dalla definizione di $\overline{C}$ seguirebbe $c \in \overline{C}$; se fosse $c \in \overline{C}$ dalla definizione di C seguirebbe $c \in C$.
Entrambe le possibilità portano a situazioni contradditorie e quindi si deve concludere $\lceil \mathbb{N} \triangleleft\!\!\!\rightarrow\!\!\!\triangleright \mathfrak{P}(\mathbb{N}) \rceil = \emptyset$ ▮

Osserviamo che abbiamo svolta una tipica dimostrazione per assurdo, chiaramente molto diversa da tutte le dimostrazioni costruttive; in effetti la natura dell'enunciato non consente che esso sia ottenuto con una costruzione effettiva.

B42g.06 Due insiemi che si possono porre in corrispondenza biunivoca si dicono **insiemi equicardinali**.

Sono equicardinali gli insiemi finiti caratterizzati da uno stesso cardinale n; risulta utile estendere la nozione di cardinale a tutti gli insiemi.
Abbiamo quindi definito **cardinale di un insieme** E, e denotiamo con $\mathsf{Card}(E)$ o con $|E|$, la classe di equicardinalità nella quale E si colloca.

Agli insiemi numerabili si attribuisce il cosiddetto **cardinale del numerabile** denotata $\aleph_0$, letta "alef con 0".
Agli insiemi come $\mathfrak{P}(\mathbb{N})$ e agli insiemi che si possono porre in biiezione come l'insieme dei numeri esprimibili con una successione (numerabile) di bits si attribuisce il **cardinale del continuo** denotata $\aleph_1$, da leggere "alef con 1".
La collezione dei cardinali in generale si può considerare un'estensione dell'insieme dei numeri naturali; queste nuove entità quindi sono state chiamate **numeri transfiniti**.

Per i cardinali di due insiemi finiti A e B con $A \subset B$ si ha la disuguaglianza $|A| < |B|$. Dato che in $\mathbb{N}$ e in ogni insieme numerabile si può individuare un sottoinsieme di n elementi, con n naturale arbitrario, risulta significativo scrivere $\forall n \in \mathbb{N} \;\vdots\; n < \aleph_0$.

Osserviamo poi che $\{n \in \mathbb{N} :| \; \{n\}\}$ è un sottoinsieme numerabile di $\mathfrak{P}(\mathbb{N})$.
Inoltre ogni insieme S equicardinale con $\mathfrak{P}(\mathbb{N})$ possiede un sottoinsieme proprio numerabile: per ogni $\gamma \in \lceil \mathfrak{P}(\mathbb{N}) \triangleleft\!\!\longrightarrow\!\!\triangleright S \rceil$ come sottoinsieme numerabile si può assumere $\{n \in \mathbb{N} :| \; \gamma(\{n\})\}$.
Per esempio un sottoinsieme numerabile dell'intervallo reale $[0, 1]$ è $\{1, 1/2, 1/4, 1/8, ..., 1/2^n, ...\}$, sottoinsieme corrispondente alla biiezione $\gamma := \left\lceil \{n\} \mapsto \frac{1}{2^n} \right\rceil \dot{\cup} \; . \; . \; . \; .$
Queste considerazioni giustificano l'enunciato $\aleph_0 < \aleph_1$.

B42g.07 È naturale chiedersi se si possono individuare insiemi con cardinali superiori ad $\aleph_1$.
In effetti si possono considerare insiemi con cardinaledate da num transfiniti costituenti una successione illimitata totalmente ordinata

$$\aleph_0 < \aleph_1 < \aleph_2 < ... < \aleph_n < \; . \; . \; . \; .$$

A questo si perviene attraverso la semplice generalizzazione della dimostrazione del teorema di Cantor che segue.

B42g.08 **Teorema** Consideriamo un insieme E e il relativo insieme delle parti $\mathfrak{P}(E)$; quale che sia il suo cardinale

$$\lceil E \triangleleft\!\!\longrightarrow\!\!\triangleright \mathfrak{P}(E) \rceil = \emptyset \; .$$

Dim.: Supponiamo che esista una biiezione $\beta \in \lceil E \triangleleft\!\!\longrightarrow\!\!\triangleright \mathfrak{P}(E) \rceil$. Consideriamo allora l'insieme $C := \{x \in E :| \, x \notin \beta(x)\}$ ed il suo complementare $\overline{C} := \{x \in E :| \, x \in \beta(x)\}$.

Dato che $C \in \mathfrak{P}(E)$, dovrebbe trovarsi in E un c tale che $C = \beta(c)$. Ci chiediamo allora se questo elemento di E appartiene a C o meno.

Se fosse $c \in C$ dalla definizione di $\overline{C}$ seguirebbe $c \in \overline{C}$; se fosse $c \in \overline{C}$ dalla definizione di C seguirebbe $c \in C$. Entrambe le possibilità portano a situazioni contraddittorie e quindi si ottiene l'enunciato ▮

Dimostriamo ora che anche **Rel**$\mathbb{N}$, l'insieme delle relazioni entro $\mathbb{N}$, ha il cardinale del continuo.

Ogni relazione entro $\mathbb{N}$ si può rappresentare fedelmente come matrice binaria di profilo $\mathbb{N} \times \mathbb{N}$ che presenta uno e un solo uno in ogni linea verticale.
A ciascuna di queste matrici si associa biunivocamente una sequenza-N binaria.
Quindi $|\mathbf{Rel}(\mathbb{N})| = |\lceil \mathbb{N} \longmapsto \mathbb{B} \rceil| = |\mathfrak{P}(\mathbb{N})| = \aleph_1$ ▮

B42g.09 Coroll.: Anche insiemi di funzioni come $\lceil \mathbb{N} \longmapsto \mathbb{N} \rceil$ o $\lceil \mathbb{P} \triangleleft\!\!\longrightarrow\!\!\triangleright \mathbb{P} \rceil$ hanno cardinale $\aleph_1$.

Dim.: Infatti, dato che si tratta di sottoinsiemi propri di $Rel(\mathbb{N})$, il loro cardinale è al più $\aleph_1$.
Per confrontare $\lceil \mathbb{N} \longmapsto \mathbb{N} \rceil$ e $\mathfrak{P}(\mathbb{N})$ si osserva che gli elementi di questi insiemi si possono porre in corrispondenza biunivoca con matrici binarie di profilo $\mathbb{N} \times \mathbb{N}$ aventi un solo 1 su ogni verticale, quelle relative al secondo insieme costituendo un sottoinsieme proprio dell'insieme costituito da quelle relative al primo. Quindi il cardinale di $\lceil \mathbb{N} \longmapsto \mathbb{N} \rceil$ è almeno $\aleph_1$.

Per confrontare $\lceil \mathbb{N} \triangleleft\!\!\longrightarrow\!\!\triangleright \mathbb{N} \rceil$ con $\mathfrak{P}(\mathbb{N})$, si osserva che gli elementi del primo insieme si possono porre in corrispondenza suriettiva con le sequenze-N binarie associando a ogni intero naturale n il valore del suo equivalente modulo 2, mentre gli elementi del secondo sono in corrispondenza biunivoca con le sequenze-N binarie.
Quindi il cardinale di $\lceil \mathbb{N} \triangleleft\!\!\longrightarrow\!\!\triangleright \mathbb{N} \rceil$ è almeno $\aleph_1$ ▮

B42g.10 Si dimostra anche che se il cardinale di un certo insieme E è $\aleph_i$, $\mathbf{Rel}(E)$, $\lceil E \longmapsto E \rceil$ e $\lceil E \triangleleft\!\!\longrightarrow\!\!\triangleright E \rceil$, come $\mathfrak{P}(E)$, hanno cardinale $\aleph_{i+1}$.

Mediante le costruzioni riguardanti il passaggio da un insieme all'insieme delle sue parti, delle relazioni, delle endofunzioni e delle permutazioni il cardinale passa al numero transfinito con indice aumentato di 1.

È naturale chiedersi se esistono insiemi infiniti aventi cardinale non facente parte della sequenza degli $\aleph_i$.
Attualmente a questa domanda non si sa dare risposta.

L'esposizione in `https://www.mi.imati.cnr.it/alberto/` e `https://arm.mi.imati.cnr.it/Matexp/matexp_main.php`